Information Sharing Environment
Interim Implementation Plan

Prepared Pursuant to
Intelligence Reform and Terrorism Prevention Act of 2004
Section 1016(e)

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JAN 2006		**00-01-2006 to 00-01-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Sharing Environment Interim Implementation Plan	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ISC Secretariat,2100 K Street NW,Washington,DC,20511**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**45**	

TABLE OF CONTENTS

Preface

This document, developed in consultation with the Information Sharing Council (ISC), represents an interim implementation plan and serves as a roadmap for developing the comprehensive implementation plan for the ISE, which is expected to be submitted to the Congress in July 2006.

In the past four years, the Administration has taken significant steps toward advancing our ability to share terrorism information. Through Executive Orders 13311 and 13356, the Administration laid the foundation for improving information sharing. On October 25, 2005, President Bush added to this foundation by publishing Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans.* That order makes clear the President's intent to ensure that the heads of all Federal departments and agencies who "possess or acquire terrorism information shall promptly give access to the terrorism information to the head of each other agency that has counterterrorism functions" unless directed otherwise by the President or are forbidden from doing so because of statutory and other legal restrictions.

In parallel with these efforts, Congress enacted three laws providing the U.S. Government with greater authority for collecting, analyzing, and disseminating terrorist information: the USA PATRIOT Act of 2001, the Homeland Security Act of 2002, and the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). In addition, the Administration has adopted the majority of information sharing recommendations put forth by the *Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.*

Today, the sharing of terrorism information takes place within multiple sharing environments within individual communities of interest such as law enforcement; homeland security; State, local, and tribal; defense; intelligence; diplomatic, and the private sector. Over time, each of these communities of interest has developed its own unique policies, rules, guidelines, standards, architectures, and systems to meet its specific mission requirements. In every case, the goal was delivery of functionality and capabilities to accomplish their specific mission requirements. As a result, the current information sharing environment is not as integrated, interconnected, or as robust as the nation requires. The challenge, therefore, is to transform the current ISE to one that better facilitates and expedites access to terrorism information and enables the sharing and integration of information across appropriate Federal, State, local, and tribal governments and private sector entities.

The vision for tomorrow's ISE consists of creating the conditions by which information can be accessed across agency and jurisdictional boundaries and between the Federal Government and its State, local, tribal and private sector partners in a timely, efficient, and frictionless manner while protecting the information privacy and other legal rights of Americans. The ISE will leverage existing information sharing capabilities to the maximum extent possible, build a centralized governance structure and a decentralized environment, and focus on more than intelligence information. This transformation will occur through a series of directed incremental steps.

Section 1016 of IRTPA provides for a phased development process for the ISE -- the appointment of the Program Manager (PM), the Program Manager's issuance of a Preliminary Report, and the issuance of Presidential Guidelines and Requirements address the first three phases. Section 1016(e) represents the fourth and perhaps the most important phase of the

development process, by requiring an implementation plan for the ISE that addresses eleven requirements.

These requirements for the implementation plan call for detailed answers that can only be provided after significant coordination between the PM and all departments and agencies, as it is the departments and agencies that ultimately are responsible for implementing the ISE. Adding to the complexity of this task is the fact that the needs of State, local, and tribal governments and private sector entities must be taken into account as well. Moreover, several of the descriptions and policies required for the implementation plan are being developed under the direction provided by the Presidential Guidelines and Requirements. Thus the report being submitted at this time is an interim report – a necessary step in an incremental, iterative process to achieve a more robust and more effective ISE.

My office, under the leadership of the Director of National Intelligence (DNI), is committed to creating an effective information sharing environment that meets the needs and requirements of all levels of government and the private sector: a national ISE. This task will include the development of policies that will enable individual Federal agencies and key partners to begin to adopt practices that reflect effective terrorism information sharing capabilities and procedures. State, local, and tribal governments and private sector entities must be full partners in this effort. I look forward to the continued support of Congress as we collectively begin to make incremental progress in providing decision makers access to the best possible information to enable the best possible decision making to protect this Nation from terrorist attacks.

John A. Russack
Program Manager
Information Sharing Environment

1 Purpose

Section 1016 of *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA)[1] calls for the President to "create an Information Sharing Environment (ISE) for the sharing of terrorism information"[2] among Federal, State, local, and tribal governments, and, where appropriate, with the private sector entities and foreign allies, in a manner consistent with the protection of homeland and national security and with the protection of information privacy rights and other legal rights of Americans. To assist in the development of the ISE, IRTPA provides for the designation of a Program Manager (PM) "responsible for information sharing across the Federal Government."[3]

As the President recently noted in his Message to Congress, creating the ISE is a "difficult and complex task."[4] The Congress also recognized the difficulty of translating generalized calls for improved information sharing into a functioning and fundamentally altered system when it drafted Section 1016 to provide for a phased development process, with periodic reporting to the Congress.[5] One such phase is the development of the Implementation Plan for the ISE.[6] This document, developed by the PM in consultation with the Information Sharing Council (ISC), represents an interim implementation plan and serves as a roadmap for developing the comprehensive Implementation Plan for the ISE, which is expected to be submitted to the Congress in July 2006. This interim plan identifies a vision and strategy for the development of the ISE, and describes the corresponding activities to be undertaken by the PM, Federal departments and agencies, State, local, and tribal governments, and private sector entities.

[1] Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004) [hereinafter IRTPA].
[2] *See* IRTPA at §1016 (a) and (b). "Terrorism information" is defined as, "all information, whether collected, produced, or distributed by intelligence, law enforcement, military, homeland security, or other activities relating to: (A) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or material support, or activities of foreign or international terrorist groups or individuals, or of domestic groups or individuals involved in transnational terrorism; (B) threats posed by such groups or individuals to the United States, United States persons, or United States interests, or to those of other nations; (C) communications of or by such groups or individuals; or (D) groups or individuals reasonably believed to be assisting or associated with such groups or individuals." *Id*. at (a)(4).
[3] *See* IRTPA, § 1016 (f).
[4] Message to the Congress of the United States, December 16, 2005.
[5] Pages S11972-S11974 of the Congressional Record, December 8, 2004 - "INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004--CONFERENCE REPORT".
[6] *See* IRTPA, § 1016 (e).

2 Introduction

2.1 Today's Environment for Sharing Terrorism Information and Why It Needs Improvement

The 9/11 attacks demonstrated that terrorists have the desire and capabilities to carry out attacks with catastrophic consequences within the United States. Moreover, it exposed substantial deficiencies in the sharing of terrorism information among Federal, State, local, and tribal authorities and the private sector. Specifically, the *Final Report of the National Commission on Terrorist Attacks Upon the United States*[7] identified several instances in which potentially useful information was (1) available but no one knew to ask for it, (2) distributed only in compartmented channels, or (3) requested but withheld due to a determination that sharing was not permitted.[8]

Legislative changes and executive orders have reduced some of the barriers to information sharing, and progress has been made in strengthening the government's sharing capabilities, while protecting the information privacy rights and other legal rights of Americans. However, the current environment that supports the sharing of terrorism information remains overly complex and not sufficiently robust to meet the needs of its users. This environment includes a variety of organizational structures, policies, business rules, and technologies for gathering, analyzing and sharing terrorism information. This situation can best be characterized as a collection of multiple sharing environments within separate but overlapping communities, each providing important and unique contributions to the war on terror, including law enforcement; homeland security; intelligence; defense; diplomatic; State, local, and tribal; and the private sector.

Currently, departmental and interagency communities of interest facilitate terrorism information sharing within a specific discipline or a particular component of the counterterrorism community, with the goal of making information and capabilities available to accomplish mission-specific requirements. In this regard, many of these entities have achieved some degree of success. The result, however, is the emergence of multiple, mission-specific information sharing systems, with disparate policies, business rules, cultures and technologies, which has unintentionally impeded the sharing of terrorism information between the various communities and across counterterrorism domains. This situation is exacerbated by the fact that the counterterrorism roles, responsibilities, and missions of departments, agencies and non-Federal entities overlap, are unclear and have interdependencies that are not fully understood. These factors result in conflicting requirements that obstruct consensus on which policies, business rules and systems best facilitate the sharing of terrorism information.

The ISE of the future must transform, integrate and connect existing elements into a cohesive framework by providing common policies, guidelines, systems and architecture. Leveraging existing initiatives will be critical to getting this task done in an expedited manner. The challenge herein is that terrorism information is not limited to intelligence. The counterterrorism mission will require the integration of classes of information from multiple communities of interest. Each of these classes of information possesses its own unique legal requirements, business rules, technical architectures, standards and capabilities. The success of the effort will be directly related to the commitment that each participant makes to foster a culture that allows for the collective to be greater than the sum of its parts.

[7] THE 9/11 COMMISSION REPORT (2004), available at http://www.9-11commission.gov/report/index.htm.
[8] *See id*.

2.2 Recent Accomplishments Enabling Information Sharing Efforts

The Congress and the Administration have taken a number of steps to advance the nation's ability to share terrorism information more effectively, including the enactment of the USA PATRIOT Act of 2001,[9] the Homeland Security Act of 2002,[10] and IRTPA of 2004. Through Executive Orders 13311,[11] 13354[12], and 13356,[13] President Bush further established a foundation for improving terrorism information sharing, and on October 25, 2005, the President built upon this foundation with Executive Order 13388, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*.[14] This order reflects and conforms to the information sharing provisions in Section 1016 of IRTPA and formed the Information Sharing Council by designating the Program Manager as the chair. Since the issuance of Executive Order 13388, departments and agencies have approved a charter, which further outlines how the ISC will fulfill its statutory purpose of assisting and advising the President and the PM in carrying out their duties under Section 1016 of IRTPA; heads of departments and agencies have designated their representative to the ISC; and the ISC has met to consult on this Interim Implementation Plan.[15]

The PM's statutory responsibilities for the planning, oversight and management of the ISE allow for the authorities and directives described in the paragraph above to be implemented in a coordinated manner – which is crucial to the ISE transformation process. Since the appointment of the PM in April 2005, a number of steps have established the support structure necessary for the PM to address the existing challenges and assist in the creation of the Information Sharing Environment. These steps included:

- The Office of Management and Budget (OMB), as part of the fiscal year 2006 (FY2006) budget process, conducting a Budget Data Request to departments and agencies as a first step in compiling a list of Federal information technology investments that support terrorism information sharing (April-September 2005);
- Formally establishing and housing the Office of the PM (June-December 2005);
- Establishing an Information Sharing Policy Coordination Committee (ISPCC), co-chaired by the Homeland Security Council (HSC) and the National Security Council (NSC) with the PM as a member, to address policy information sharing issues, including departments' and agencies roles and responsibilities (June 2005);
- Issuing the Program Manager's *"Preliminary Report on the Creation of the Information Sharing Environment,"* which provides a description of the technological, legal and policy issues presented by the creation of the ISE (June 2005);
- Issuing a Request for Information (RFI) to industry for Electronic Directory Services (EDS) as required by IRTPA (August 2005) and determining the appropriate EDS development activities (November 2005);

[9] UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 24, 2001).
[10] Pub. L. No. 107-296, 116 Stat. 2135 (Nov. 25, 2002).
[11] HOMELAND SECURITY INFORMATION SHARING, 68 Fed. Reg. 45149 (July 29, 2003).
[12] NATIONAL COUNTERTERRORISM CENTER, 69 Fed. Reg. 53589 (Aug. 27, 2004).
[13] Strengthening the Sharing of Terrorism Information to Protect Americans, 69 Fed. Reg. 53599 (Aug. 27, 2004).
[14] 70 Fed. Reg. 62023 (Oct. 27, 2005). This Order amends Exec. Order No. 13311 and revokes Exec. Order No. 13356.
[15] *Id.*

- Issuing Executive Order 13388, creating the Information Sharing Council and identifying the PM as the chair (October 2005); and
- Holding the initial meeting, and subsequent follow-on meetings, of the Information Sharing Council (November-December 2005).

Implementing a robust ISE requires leveraging all of these accomplishments and authorities. Specifically, rules must be established to govern how and under what conditions information will flow across interdepartmental, interagency and intergovernmental boundaries, as well as who can authoritatively act on that information. To facilitate this process, the President recently issued guidelines and requirements, which represent a significant step forward in the establishment of the ISE. The implementation of these guidelines and requirements will:[16]

- Clarify roles and authorities across executive departments and agencies;
- Implement common standards and architectures to further facilitate timely and effective information sharing;
- Improve the Federal Government's terrorism information sharing relationships with State, local, and tribal governments, the private sector, and foreign allies;
- Revamp classification and marking systems, as they relate to sensitive but unclassified information;
- Ensure that the information privacy rights and other legal rights of Americans are protected in the development and implementation of the ISE; and
- Ensure that departments and agencies promote a culture of information sharing by assigning personnel and dedicating resources to terrorism information sharing.

While the task ahead is complicated, the fundamental principles are in place to guide future ISE development.

2.3 Section 1016(e) Requirements

As noted above, Section 1016 of IRTPA provides for a phased development process for the ISE -- the appointment of the Program Manager, the Program Manager's issuance of a Preliminary Report, and the issuance of Presidential guidelines and requirements address the first three phases. Section 1016(e) represents the fourth and perhaps the most important phase of the development process by requiring an implementation plan for the ISE that addresses the following eleven requirements:

(1) A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards;

(2) A description of the impact on enterprise architectures of participating agencies;

(3) A budget estimate identifying the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE;

[16] Memorandum to the Heads of Executive Departments and Agencies, Subject: *Guidelines and Requirements in Support of the Information Sharing Environment,* (December 16, 2005).

(4) A project plan for designing, testing, integrating, deploying, and operating the ISE;

(5) The policies and directives that govern the content and usage of the ISE, as well as the metrics and enforcement mechanisms that will be utilized;

(6) Objective, system-wide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE;

(7) A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized;

(8) A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE;

(9) The recommendations of the PM, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other information;

(10) A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE; and

(11) The recommendations of the PM, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of PM should continue to remain in existence.

These requirements call for detailed answers that can only be provided after significant coordination between the PM and the departments and agencies, as it is the departments and agencies that ultimately are responsible for implementing the ISE. Adding to the complexity of this task is the fact that the needs of State, local, and tribal governments and private sector entities must be taken into account as well. Moreover, several of the descriptions and policies required for the implementation plan are being developed under the direction provided by the Presidential guidelines and requirements. Accordingly, this is an interim implementation plan – a necessary step in an incremental, iterative process to achieve a successful ISE. This plan provides a vision and strategy for the implementation of the ISE, and addresses, at least in part, all of the Section 1016(e) reporting requirements.

In developing this vision and strategy for implementation, it became apparent that establishing an ISE represents a challenging and complex undertaking for the following reasons:

- No single organization is solely in charge of, or responsible, for the implementation of the ISE, yet each participating organization has a role and a stake;
- Mission success depends on a high degree of cooperation, coordination and alignment among a diverse set of participants;
- The ISE must align with, complement and support the individual missions of the ISE participants. The nation's terrorism information infrastructure cannot be separated from existing infrastructure supporting other mission priorities;

- Organizations are expected to use existing resources to meet the demands of the counterterrorism mission, creating competition for resources;
- New business rules must be established to create cross-organizational operational efficiencies; and
- Effective sharing will require changing the cultures within organizations and redefining the policies, processes and technical systems that currently exist within the counterterrorism operating environment.

Members of the ISC recognize the need to design a robust concept of operations before submitting a comprehensive Implementation Plan. The concept of operations will identify impediments and accompanying solutions to ensure the successful evolution of the ISE. Moreover, it will provide a platform to encourage the communities participating in the ISE to adopt a common lexicon and shared philosophical approach regarding how the sharing of terrorism information best supports national efforts to detect, prevent, respond to and recover from acts of terrorism. Prior to the release of the comprehensive Implementation Plan, there must be a clear delineation of roles and responsibilities, identified deliverables, and corresponding performance measures to allow for the implementation of effective solutions that meet IRTPA requirements. To accomplish these objectives, this Interim Implementation Plan outlines a roadmap for Federal, State, local, and tribal governments and private sector entities to arrive at a common understanding of the solutions that are necessary and achievable within an evolving ISE.

3 Interim Implementation Plan

3.1 A Vision for the Future

IRTPA calls for the creation of an ISE for terrorism information in a manner consistent with national security and the information privacy and other legal rights of Americans. In accordance with IRTPA, the ISE will reflect the combination of policies, procedures and technologies connecting the resources (information, organizations, services and personnel) of the Federal, State, local, and tribal governments, and as appropriate, the private sector and foreign allies, to ensure terrorism information sharing, access and collaboration among users is readily available. Further, the President has directed that the development of the ISE take into account the counterterrorism missions, roles, and responsibilities of executive departments and agencies, and that State, local, and tribal governments, law enforcement agencies, and the private sector have the opportunity to participate as full partners in the ISE. In so doing, there must be a clear understanding that in some cases, ISE participants fulfill their counterterrorism responsibilities within a broader law enforcement, public safety or public health context. Additionally, there must be an understanding that any actionable terrorism information, where appropriate and possible, should include unclassified content that can be utilized at the local level.

Therefore, the ISE, created and maintained in full partnership by all levels of government and, as appropriate, with the private sector, will effectively support the detection, prevention, disruption, preemption and mitigation of the effects of terrorism activities against the territory, people and interests of the United States of America.[17] It will accomplish this by enabling the trusted exchange of terrorism information between and among appropriate Federal, State, local, and tribal governments and private sector entities at multiple security levels,[18] while also safeguarding the information, protecting sources and methods and the information privacy rights and other legal rights of Americans in the conduct of these activities.[19]

To achieve these goals, the ISE will have the following attributes: [20]

- Connects existing systems, where appropriate; provides no single points of failure; and allows users to share information among agencies, between levels of government, and, as appropriate, with the private sector;
- Ensures direct and continuous online electronic access to information;
- Assures the availability of information in a form and manner conducive to its use in analysis, investigations and operations;
- Builds upon existing systems' capabilities currently in use across the government;
- Employs an information access management approach that controls access to data rather than just systems and networks, without sacrificing security;
- Incorporates strong mechanisms to enhance accountability and facilitate oversight, including audits, authentication and access controls;
- Facilitates the sharing of information at and across all levels of security;
- Allows authorized users to locate people and information; and

[17] *See* Exec. Order No. 13388, § 1(a)(i) (Oct. 25, 2005).
[18] *See id*. at § 1(a)(ii) and 1(a)(iii).
[19] *See id.* at § 1(a)(iv) and 1(b).
[20] *See* IRTPA, § 1016(b)(2)

- Incorporates protections for the information privacy rights and other legal rights of Americans.

While a large amount of terrorism information already is stored electronically in systems, many users are not connected to those systems. In addition, there remains an unknown quantity of relevant information not captured and stored electronically. Thus, the information about terrorists, their plans and activities is fragmentary. The ISE will connect disparate electronic storehouses so we can take advantage of what already exists. Additionally it will provide mechanisms for capturing and providing access to terrorism information currently not available electronically.

Terrorism information encompasses a wide array of information with disparate characteristics and uses. In today's environment, the relevant community of information collectors, analysts and users extends beyond the Federal government to include State, local, and tribal governments, foreign entities, and the private sector. Information available to any single member of the ISE may prove essential to understanding the current terrorism threat picture. Accordingly, the ISE must provide a framework to determine the appropriate means and scope of access to the many different categories of terrorism information.

Finally, along with improving terrorism information access, the ISE must also incorporate abilities to measure and account for the value of the information being shared and ensure that the information being provided has the greatest impact on the nation's ability to address immediate and emerging terrorist threats and events. To do so, the ISE will fully incorporate performance and accountability measures that directly relate to reducing the risk of terrorism today and in the future.

To realize these attributes, the ISE will provide a disciplined, integrated and trusted structure for the creation, protection, dissemination and use of actionable terrorism information across all related communities. Each of these communities—law enforcement, homeland security, State, local, and tribal, defense, intelligence, diplomatic, and the private sector—provides important and unique contributions to the war on terror, and each presents its own set of requirements on the proposed environment.

The ISE must, therefore, provide capabilities that allow terrorism information to be integrated so users across all the communities can better detect threats relevant to their missions. At the same time, the ISE policies, procedures and technologies must fully support the specific functions that each community uses to achieve its mission. To do this, the ISE will, at a minimum, provide the following key capabilities for all communities comprising the environment:

- Easier User Access. Users face a wide variety of systems and tools with different policies, procedures and access controls. The environment must simplify access for users regardless of their point of entry into the environment.
- Security and Privacy Safeguards. The environment must protect privacy and civil liberties while permitting access to appropriate data from the public and private sectors.
- Information Discovery and Search. Currently, users typically must know where information is likely to be located and then search for it using query mechanisms that assume they know what questions to ask. The environment will allow information users to discover the information they need without knowing its location or even if the information exists.
- Information Access. Actionable information does not always get to the people who need it when they need it. The environment will enable users to get the information they need whether it is pulled as a result of a search or automatically pushed to them.

- Knowledge Extraction. There is too much information and there are too many interrelationships to link disparate information, and draw real-world actionable conclusions from the enormous amount of data available. The environment must be able to work with all sorts of information, from highly structured relational databases, to semi-structured materials, to unstructured textual content as well as provide tools to enable users to make sense of the information they obtain.
- Collaboration. Users need to be able to collaborate more effectively with other users in order to make the best use of the information provided to them. The environment will support the creation of ad-hoc collaboration groups, and incorporate tools to enable multiple people to communicate on areas of mutual interest across organizational boundaries.

Successful implementation and continuous improvement of Electronic Directory Services (EDS) is a critical component to achieving these ISE capabilities. EDS must be fully integrated and connected to the ISE, with multiple directory services working together and sharing information. This will ensure that people and organizations have easier user access and collaboration capabilities, and service and data directories are supporting information discovery and search, information access and knowledge extraction.

Success of the ISE also depends upon the creation and incremental improvement of these capabilities while protecting the information privacy rights and other legal rights of Americans in a manner that provides transparency to the public about the purpose and operation of the ISE. The ISE must address the accuracy of data about individuals, provide appropriate controls to access information about individuals, ensure the appropriate use of such information, and provide an appropriate mechanism for individuals to request corrections to errors of any kind.

The ISE will improve the United States' ability to produce and disseminate accurate, timely and validated terrorism information, and thereby enhance the nation's ability to address immediate or emerging terrorist threats and events. It will continually evolve as it adapts to changes in the terrorist threat, national risks and mission requirements.

3.2 Implementation Approach

Given the complexity and size of the ISE, an incremental and iterative implementation approach—fully grounded in the overall ISE vision—offers the most practical and cost efficient strategy to achieve the vision of the ISE. This type of approach, instead of a top-down approach, enables a continuous assessment and integration of programs, evolution of an ISE architecture, and timely performance monitoring and resource management to achieve the long-term vision and goals of the ISE.

To respond to the requirements in Section 1016 of IRTPA, ISE implementation will be based on a three-pronged strategy:

- Implementation of Presidential Guidelines and Requirements;
- Support and augmentation for existing information sharing environments, such as the National Counterterrorism Center (NCTC); and
- A process for integrating the Presidential Guidelines and Requirements with the needs of the broader ISE, addressing overall ISE functions, capabilities, resources, conceptual design, architecture, budget, and performance management.

A view of the implementation approach is depicted in Figure 3.1.

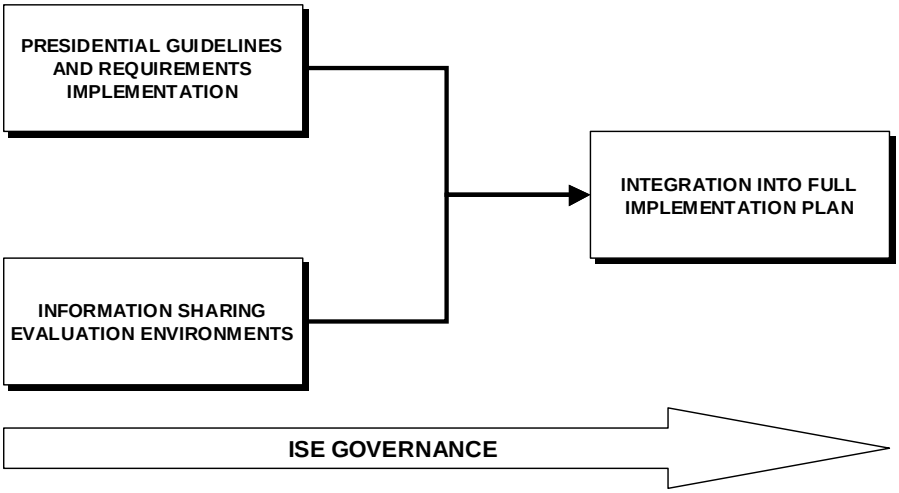

Figure 3.1 ISE Implementation Approach

3.2.1 Implementation of Presidential Guidelines and Requirements

As discussed in Chapter 1, the guidelines and requirements set forth in the December 16, 2005 Presidential memorandum include specific actions and deliverables that address critical issues affecting the design and implementation of the ISE. Collectively, they provide a roadmap by which the PM, ISC and Federal departments and agencies will address a number of longstanding information sharing issues. The specific tasks, timelines, accountability and deliverables associated with each guideline and requirement are detailed in Section 3.5. Existing and newly established working groups already have begun working on the assigned tasks.

3.2.2 Information Sharing Evaluation Environments

Individual counterterrorism missions require accessing information from varying sources with differing granularity and classification levels. Given the variety of operational missions that rely on terrorism information, ISE implementation must be flexible and adaptable. Accordingly, effecting substantive improvements in the flow of information requires a pragmatic approach to evaluate, prioritize, propose and implement solutions.

ISE implementation will be grounded in practical applications in order to identify requirements, performance elements, capabilities, and standards. As discussed below, the identification of information sharing evaluation environments creates opportunities to address these issues (and others as they arise) and make immediate improvements to terrorism information sharing.

Several mission-specific organizations already operate their own information sharing environments that encompass a number of the attributes and capabilities of the larger ISE, reflecting both progress and impediments to information sharing. These existing, individual environments enable the development and application of policies, business processes, procedures and technology solutions that will provide a baseline for positive change across the ISE.

In order to extract lessons learned and apply them to the ISE as a whole, it is essential to identify environments representative of broader issues affecting the entire ISE. Initially, evaluation activities will be focused on at least two environments—one or two that are central to sharing terrorism information across the Federal Government, and the other addressing the all-

way sharing of information between the Federal Government, State, local, and tribal governments and private sector entities.

The NCTC will serve as one of the initial Federal Government information sharing evaluation environments. The NCTC was selected because it is the primary organization in the U.S. government for analyzing and integrating all information pertaining to terrorism and counterterrorism.[21] The missions of the NCTC include:

- Ensuring that agencies, as appropriate, have access to and receive all-source information support needed to develop and execute their counterterrorism plans or perform independent alternative analysis; and
- Serving as the central and shared knowledge bank on known and suspected terrorists and international terror groups, as well as their activities, goals, strategies, capabilities and networks of contacts and support.[22]

Given its statutory role in the Federal Government's counterterrorism activities, the NCTC offers the unique opportunity for application, monitoring, and assessment of terrorism information flow across the Federal Government.

In the recently issued Memorandum to Heads of Executive Departments and Agencies on *Guidelines and Requirements in Support of the Information Sharing Environment*, the President directed that State and local governments "must have the opportunity to participate as full partners in the ISE". Over the past few years, a number of initiatives have emerged to address the complex challenge of improving Federal, State and local information sharing. The Department of Homeland Security (DHS) and the Department of Justice (DOJ) have already reached out extensively to State, local, and tribal governments and private sector entities -- this includes work with statewide and major urban area information fusion centers. In addition, since January 2005, two Federal Advisory Groups—the Global Justice Information Sharing Initiative and the Homeland Security Advisory Council—comprised principally of State and local officials have worked in consultation with officials from the DHS and DOJ to develop guidelines to assist in the implementation of statewide and major urban area information fusion centers. The ISE will build on the work of these groups. Further, to ensure that State and local governments have the opportunity to be partners in the development and implementation of the ISE, DHS and DOJ in partnership with State and local representatives, will identify one or more environments run by states and major urban areas for evaluation of the effectiveness of the flow of terrorism information between Federal, State and local governments and the private sector.

3.2.3 Integrating Results into the Broader ISE Implementation

Although the implementation of the Presidential Guidelines and Requirements, as well as the solutions resulting from the information sharing evaluation environments, will demonstrate concrete progress against real-world problems, it is also essential that these activities allow for an overarching ISE architecture that includes associated functions, capabilities, design and standards. ISE participants must be able to identify the specific impacts to their respective enterprise architectures and to plan for short- and long-term budget adjustments. Accordingly, a major part of the implementation process will provide the means to address broader ISE integration issues relating to budget, performance management and ISE architecture. In addition, it will form the basis for the project plan for designing, testing, integrating, deploying and operating the ISE as required by IRTPA. Specific topics of the broader ISE integration are addressed in Section 3.6 of this plan.

[21] *See* IRTPA, § 1021 (excepting intelligence pertaining to domestic terrorism and counterterrorism).
[22] *See id*.

The ISE implementation approach for integrating results into the broader ISE includes the following steps:

- Identify specific information sharing issues and impediments from the working groups associated with the implementation of the Presidential Guidelines and Requirements and the evaluation environments;
- Prioritize these issues using criteria that will emphasize the potential application to or impact on the broader ISE, and create a list of requirements based on the prioritized issues;
- Develop options and recommendations for solutions that entail new or modified policies, processes, procedures and technology, along with estimated resource impacts;
- Assess how each recommendation will be incorporated into the overall ISE implementation plan, specifically addressing the requirements in Section 1016(e) of IRTPA;
- Present these recommendations to the ISC for decision and implementation. As discussed in Section 3.3, other elements of the ISE governance structure will be engaged if required;
- Identify and designate lead implementing department(s) or agency(s) for each approved recommendation;
- Use ISC-endorsed recommendations with their accompanying assessments to form the basis for the full ISE implementation plan. This incremental approach to the full plan will respond to the requirements of Section 1016(e) of IRTPA (see Section 3.4); and
- Measure progress and outstanding issues associated with approved ISE tasks through regular review by the ISC to enable the assessment of progress toward the realization of the ISE vision. This ongoing activity drives toward continual improvement by implementing and monitoring terrorism information sharing requirements and identifying gap solutions using new and updated ISE investments.

3.3 ISE Governance

In accordance with IRTPA, the President will "enforce the policies, directives and rules that will govern the content and usage of the ISE."[23] Under the President's authority, the PM is responsible for planning for and overseeing the implementation of, and managing, the ISE [24] In this capacity, the PM will assist, monitor and assess progress and compliance throughout the implementation phases.[25] This will be accomplished under his statutory role as the PM, and through his position as Chair of the ISC. The ISC is integral to the success of the ISE as a mechanism that will effectively support and advise the PM during implementation, as well as ensure coordination among participants for the establishment of the ISE.

In order to effectively identify and resolve issues related to the implementation of the ISE, the office of the PM has been structured with the goal of providing regular staff interaction with ISE communities. Through this interaction, the PM will attempt to resolve questions and disputes among communities, elevating any unresolved issues to the ISC for collaborative resolution. If necessary, matters may be further elevated to the ISPCC for consideration and resolution.

[23] IRTPA §1016 (b)(1)(C).
[24] *See id.* at (f)(2)(A)(i).
[25] *See id*. at (f)(2)(A)(iii).

Depicted in Figure 3.2 and described below are the specific governance responsibilities of the PM, the ISC, the ISPCC and the Privacy and Civil Liberties Oversight Board.

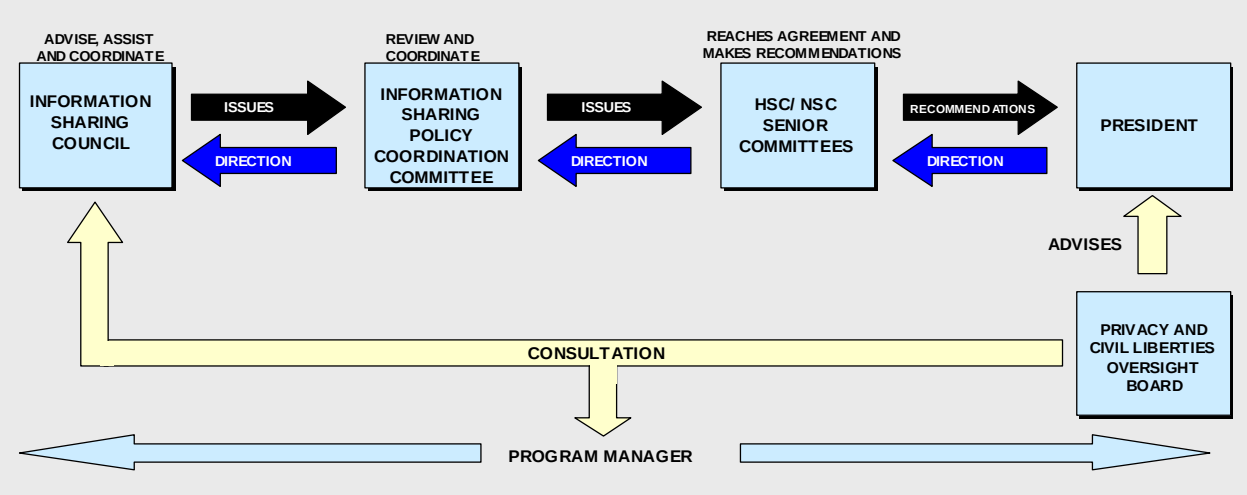

Figure 3.2 ISE Implementation Governance

3.3.1 The Program Manager

The PM will build upon current information sharing efforts across the U.S. Government, and facilitate change toward tomorrow's ISE, engaging the ISC in the implementation process through continuous communication, interaction and inclusion in decision-making processes. The PM will act as the catalyst to improve terrorism information sharing among ISE communities by working with them to remove barriers and facilitate change to improve information access. The PM's Office is currently supported by an experienced staff from across the U.S. Government. The PM also has the benefit of several advisors with expertise in specific information sharing issues, e.g., State and local information sharing and technology standards.

3.3.2 The Information Sharing Council

The ISC is an interagency forum established by Section 1016 of IRTPA and Executive Order 13388, and operating under a Charter approved by the ISPCC. It is an advisory body to the President and PM in the development of policies, procedures and guidelines necessary to implement the ISE. Additionally, it provides participants an avenue to actively engage in implementation planning and decision-making for the establishment of an effective ISE. The Council also acts as a mechanism to ensure coordination among Federal departments and agencies, and is a means for the PM to assess progress among ISE communities. The ISC was recently directed to establish two sub-committees to address State, local, and tribal as well as private sector issues. These subcommittees will be co-chaired by DHS and DOJ.

3.3.3 The Information Sharing Policy Coordination Committee

In June, the President also established the Information Sharing Policy Coordination Committee (ISPCC), which is chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC), and which has the responsibilities set forth in Section D of Homeland Security Presidential Directive-1 and other relevant presidential guidance with respect to information sharing. The ISPCC was established to address major information sharing policy issues, including the resolution of issues raised by the PM, and provide policy analysis and

recommendations for consideration by the more senior committees of the HSC and NSC systems. The PM is a member of the ISPCC.

3.3.4 Privacy and Civil Liberties Oversight Board

The Privacy and Civil Liberties Oversight Board (PCLOB) was created to ensure a system of checks and balances to protect individual privacy and civil liberties during the establishment of government efforts to protect the nation against terrorism.[26] The PCLOB is to provide advice and counsel on the development and implementation of policy to the President or to the head of any executive department or agency. Section 1016 requires consultation with the PCLOB to protect the information privacy rights and other legal rights of Americans in the development and use of the ISE. The PM and the ISC will work closely with the PCLOB to ensure that privacy and civil liberties are protected in the development and management of the ISE.

3.4 Status of IRTPA Requirements

Although an effective ISE implementation plan will ultimately address issues beyond those specifically identified in IRTPA, Section 1016(e) cites eleven specific requirements that must be addressed. This Interim Implementation Plan describes progress towards meeting ten of the requirements in Section 3.4.1, and one requirement, yet to be addressed, is discussed in Section 3.4.2. The following discussions also reference the recent Presidential Memorandum that issued guidelines and requirements that directly support the requirements of Section 1016(e). Tab A provides a detailed traceability of all eleven requirements of IRTPA, which are covered in corresponding sections or chapters within this document.

3.4.1 Progress Towards Meeting IRTPA Requirements

The following ten IRTPA requirements are currently in progress:

- Requirement 1—*A description of the functions, capabilities, resources, and conceptual design of the ISE, including standards.* This is addressed in part in Sections 3.1, 3.5.1, 3.5.2 and 3.6.1. Additional efforts, to more completely describe resources requirements and conceptual design, will be included in the comprehensive Implementation Plan for the ISE, which is expected to be submitted to the Congress in July 2006.
- Requirement 2— *A description of the impact on enterprise architectures of participating agencies.* Section 3.6.2 addresses many of the actions necessary to address this requirement.
- Requirement 3—*A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.* Information is still needed to satisfy this requirement. Section 3.6.3, however, establishes a roadmap for obtaining the information needed to satisfy this requirement.
- Requirement 5—*The policies and directives referred to in subsection (b)(1)(c)*[27]*, as well as the metrics and enforcement mechanisms that will be utilized.* The implementation of the Presidential Guidelines and Requirements described in Section 3.5 will result in almost all the actions necessary to fully satisfy this requirement. The results will be reported in the comprehensive Implementation Plan.

[26] *See id*. at § 1061 (a-c)
[27] This section requires the President to, "determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE."

- Requirement 6—*Objective system-wide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.* Section 3.6.4 outlines a process for implementing an ISE performance management program as called for in this requirement.
- Requirement 7—*A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized*. Although training issues are included in the discussion of the Presidential Requirement - *Promoting a Culture of Information Sharing,* (see Section 3.5.7), additional efforts are required before this requirement can be deemed fully satisfied.
- Requirement 8—A *description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE*. The tasks identified to respond to Presidential Guideline 5 (see Section 3.5.6) provide a roadmap for addressing this requirement.
- Requirement 9—*The recommendations of the PM, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information*. This requirement will be addressed in the comprehensive Implementation Plan (See Chapter 4)
- Requirement 10—*A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE.* The comprehensive effort planned in response to the recent Presidential Requirement – *Leveraging Ongoing Information Sharing Efforts in the Development of the ISE* (see Section 3.5.1) will address most of this requirement, although additional efforts will be necessary to address the portion of the requirement dealing with ISE infrastructure providers.
- Requirement 11—*The recommendations of the PM, in consultation with the Information Sharing Council, for a future management structure for the ISE, including whether the position of PM should continue to remain in existence*. This requirement will be addressed in the comprehensive Implementation Plan (see Chapter 4).

3.4.2 IRTPA Requirement To Be Addressed

Requirement 4 calls for *a project plan for designing, testing, integrating, deploying, and operating the ISE*. It will be necessary to gain additional practical experience with resolving operational information sharing problems before the project plan envisioned in Section 1016(e) can be developed. The implementation process, described in Section 3.2.3, will include the actions necessary to satisfy this requirement in the comprehensive implementation plan.

3.5 Tasks Associated with Presidential Guidelines and Requirements[28]

3.5.1 REQUIREMENT 1 – Leveraging Ongoing Information Sharing Efforts in the Development of the ISE

The ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively "resources") used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information.

- Task 1.1: Comprehensive assessment of existing resources pertaining to terrorism information sharing employed by individual or multiple executive departments and agencies.[29] (Leads: PM, ISC)

  Due Date: March 16, 2006

  Deliverable: Report assessing existing resources for utility and integrative potential in furtherance of the establishment of the ISE and identification of unnecessary redundancies.

- Task 1.2: Review and identify missions, roles and responsibilities of executive departments and agencies relating to the acquisition, access, retention, production, use, management, and sharing of terrorism information. (Leads: PM, Director of NCTC in coordination with relevant departments and agencies)

  Due Date: June 14, 2006

  Deliverable: Findings and recommendations for the further definition, reconciliation, or alteration of counterterrorism missions, roles and responsibilities.

- Task 1.3: Develop the policies, procedures, and architectures needed to create the ISE, which shall support the counterterrorism missions, roles, and responsibilities of executive departments and agencies. (Leads: PM, ISC)

  Due Date: December 11, 2006

  Deliverable: ISE policies, procedures, and architectures.

3.5.2 GUIDELINE 1 – Define Common Standards for How Information is Acquired, Accessed, Shared, and Used within the ISE

The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities.

- Task 2.1: Develop and issue common standards for preparing terrorism information for maximum distribution and access while safeguarding such information and protecting

[28] The December 16, 2005 Presidential memorandum on ISE guidelines and requirements is provided in Tab B. Tab C provides a table and timeline of due dates for the Interim Implementation Plan tasks, which is primarily comprised of tasks associated with the Presidential guidelines and requirements.
[29] This review will be based on the PM's ongoing effort to baseline the ISE.

sources and methods from unauthorized use or disclosure[30] (Lead: DNI in coordination with Secretaries of State, Defense, and Homeland Security and the Attorney General)

Due Date: March 16, 2006

Deliverable: Government-wide, common standards that promote the maximum distribution of and access to terrorism information, including the appropriate method for government-wide adoption and implementation of these standards[31].

- Task 2.2: Disseminate these standards for use by State, local, and tribal governments, law enforcement agencies, and the private sector, on a mandatory basis where possible and a voluntary basis where not. (Leads: Secretary of Homeland Security and the Attorney General)

  Due Date: June 14, 2006

  Deliverable: Common standards for use by Federal, State, local, and tribal governments, law enforcement agencies, and the private sector.

3.5.3 GUIDELINE 2 – Develop a Common Framework for the Sharing of Information between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector

Recognizing that the war on terror must be a national effort, State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE, to the extent consistent with applicable laws and executive orders and directives, the protection of national security, and the protection of the information privacy rights and other legal rights of Americans.

- Task 3.1: Perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing with State, local, and tribal governments, law enforcement agencies, and the private sector and recommend an appropriate sharing framework to the President.[32] (Leads: Secretary of Homeland Security and the Attorney General in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI)

  Due Date: June 14, 2006

  Deliverable: Recommended framework pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and

[30] These standards shall accommodate and reflect the sharing of terrorism information, as appropriate, with State, local, and tribal governments, law enforcement agencies, and the private sector.

[31] The DNI may amend the common standards from time to time as appropriate through the same process by which they were issued.

[32] Statewide (and major urban area) information fusion centers (regardless of whether they are called a fusion center, a Terrorism Early Warning System, an intelligence center, or otherwise) are a critical part of the ISE. Accordingly, in carrying out this task, DHS and DOJ will take steps to identify effective mechanisms to increase Federal coordination with these centers and incorporate them into the ISE. Additionally, DHS, DOJ and other relevant Federal entities will define how they plan to coordinate their domestic information and intelligence efforts with these State and major urban area fusion centers. DHS will complete a current capability assessment for each State and major urban area so as to document current capacity to carry out the fusion process. DHS will develop appropriate training, technical assistance, and will allow the use of grant resources so as to ensure that each State and urban area (as defined by the UASI program) establishes a consistent and baseline level of capacity to support the gathering, analysis, dissemination and use of terrorism information.

among Federal departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities.

3.5.4 GUIDELINE 3 – Standardize Procedures for Sensitive but Unclassified Information

To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive but Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, procedures and standards for designating, marking, and handling SBU information (collectively "SBU procedures") must be standardized across the Federal Government. SBU procedures must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State, local, and tribal governments, law enforcement agencies, and private sector entities. This effort must be consistent with Executive Orders 13311 and 13388, Section 892 of the Homeland Security Act of 2002, Section 1016 of IRTPA, Section 102A of the National Security Act of 1947, the Freedom of Information Act, the Privacy Act of 1974, and other applicable laws and executive orders and directives.

- Task 4.1: Conduct an inventory of SBU procedures, determine the underlying authority for each entry in the inventory, and provide an assessment of the effectiveness of existing SBU procedures. (Lead: All Federal departments and agencies)

  Due Date: March 16, 2006

  Deliverable: Report to the DNI on SBU inventory results. The DNI will, in turn, provide the compiled results to the Secretary of Homeland Security and the Attorney General.

- Task 4.2: Develop recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information. (Leads: Secretary of Homeland Security and the Attorney General in coordination with the Secretaries of State, Defense, and Energy, and the DNI)

  Due Date: June 14, 2006

  Deliverable: Report to the President in accordance with provisions of paragraph 2.c.(iv) of December 16, 2005 Presidential memorandum.

- Task 4.3: Develop recommendations for the standardization of SBU procedures for all types of information. (Lead: DNI in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General and in consultation with all other heads of relevant executive departments and agencies)

  Due Date: December 16, 2006

  Deliverable: Report to the President in accordance with provisions of paragraph 2.c.(iv) of December 16, 2005 Presidential memorandum.

- Task 4.4: Ensure on an ongoing basis that Presidentially-approved recommendations are fully implemented in such department or agency, as applicable. (Lead: All departments and agencies with support of PM)

Due Date: Ongoing

Deliverable: Guidance and training programs for the standardized SBU procedures.

3.5.5 GUIDELINE 4 – Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners

The ISE must support and facilitate appropriate terrorism information sharing between executive departments and agencies and foreign partners and allies. To that end, policies and procedures to facilitate such informational access and exchange, including those relating to the handling of information received from foreign governments, must be established consistent with applicable laws and executive orders and directives.

- Task 5.1: Review existing authorities and develop recommendations for sharing terrorism information with foreign partners and allies. (Lead: Secretary of State in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the DNI)

  Due Date: June 14, 2006

  Deliverable: Recommendations for appropriate legislative, administrative, and policy changes to facilitate the sharing of terrorism information with foreign partners and allies.

3.5.6 GUIDELINE 5 – Protect the Information Privacy Rights and Other Legal Rights of Americans

As recognized in Executive Order 13353 of August 27, 2004, the Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions. Accordingly, in the development and use of the ISE, the information privacy rights and other legal rights of Americans must be protected.

- Task 6.1: Review current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans, and develop guidelines to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE. (Leads: Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information)

  Due Date: June 14, 2006

  Deliverable: Recommended guidelines for Presidential approval that ensure the information privacy and other legal rights of Americans are protected in the development and use of the ISE.

- Task 6.2: Ensure that guidelines developed in Task 6.1 are fully implemented. (Lead: All departments and agencies)

  Due Date: Ongoing

  Deliverable: Appropriate personnel, structures, training, and technologies to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans.

3.5.7 REQUIREMENT 2 – Promoting a Culture of Information Sharing

Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.

- Task 7.1: Designate a senior official to provide accountability and oversight for terrorism information sharing, work with the PM, in consultation with the ISC, to develop high-level information sharing performance measures for the department or agency to be assessed no less than semiannually, and provide, through the department or agency head, an annual report to the DNI on best practices of and remaining barriers to optimal terrorism information sharing. (Leads: Federal departments and agencies)

  Due Date: March 16, 2006

  Deliverable: Memorandum designating responsible official for each department or agency.

- Task 7.2: Develop and issue guidelines, provide training and incentives, and hold relevant personnel accountable for the improved and increased sharing of terrorism information. (Leads: Federal departments and agencies)

  Due Date: June 14, 2006

  Deliverable: Departmental or agency guidelines, training, and incentives for promoting a culture of information sharing, including a performance evaluation element on information sharing to be included in employees' annual Performance Appraisal Review.

- Task 7.3: Bring to the attention of the Attorney General and the DNI any restriction contained in a rule, regulation, executive order or directive that significantly impedes the sharing of terrorism information. (Leads: Federal departments and agencies)

  Due date: Ongoing

  Deliverable: Department or agency memorandum, if applicable.

3.6 Overarching ISE Integration Tasks

In addition to describing the tasks necessary to fulfill the Presidential Guidelines and the information sharing evaluation environments, this Interim Implementation Plan outlines additional implementation strategies called for in Section 1016(e) of IRTPA. This section describes the approach to be used to develop the ISE conceptual design, including a description of functions, capabilities and resources. This section also identifies specifics tasks, timelines, accountability and deliverables associated with enterprise architecture, ISE budget, performance measurement and electronic directory services requirements.

3.6.1 ISE Functions, Capabilities, Resources and Conceptual Design

Section 3.1 identified six key capabilities that the ISE will provide: easier user access; security and privacy safeguards; information discovery and search; information access; knowledge extraction; and collaboration. These capabilities, initially developed in response to Executive Order 13356, provide a framework around which the specific issues and associated actions for ISE implementation will be aligned.

As the ISE implementation unfolds, a principal measure of success will be the extent to which the PM and ISC can show demonstrable improvement in these six areas. Each specific action leads to the delivery of a new ISE capability, and each will have some associated resource costs. The PM and ISC will be responsible for clearly identifying the resources required to complete each deliverable, and will make the appropriate tradeoffs to provide the most effective and efficient ISE.

Figure 3.3 illustrates the framework around which the conceptual design of the ISE will be developed. The design will encompass policies, processes and technologies to ensure that terrorism information can be freely and transparently shared across the three broad security domains with counterterrorism missions: sensitive compartmented information (SCI), classified collateral and SBU. Requirements for terrorism information exist in all three domains, and a primary goal of the ISE is to ensure that the cross-domain flow is accomplished smoothly and securely to support information discovery and knowledge extraction.

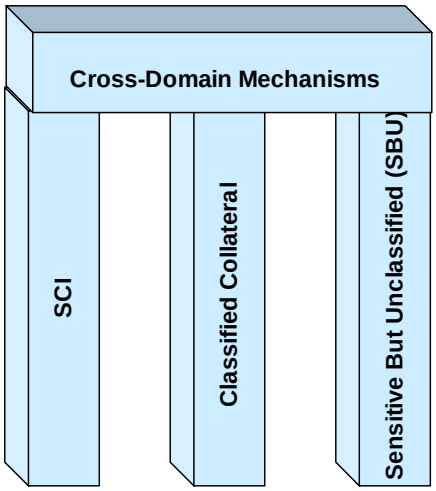

Figure 3.3 ISE Security Domains

Although cross-domain sharing takes place today, the implementations are often inefficient, typically requiring human review at the transition points. The information sharing evaluation environments will serve as platforms to test approaches for implementing trusted information exchanges across multiple domains. The ISE design will then incorporate the policies, processes and technology (controlled interfaces) used in the centers to eliminate these inefficiencies.

3.6.2 Enterprise Architecture

Agencies will have to maintain, transform or adjust their individual enterprise architectures as needed to operate within the ISE while continuing to satisfy their statutory mandates, roles and responsibilities. The ISE will link information sharing policies, business processes and technology to the Federal Enterprise Architecture (FEA) process.[33] Ultimately, the development of information sharing standards will enable agencies to operate more efficiently and effectively in fulfilling their missions through the reuse of technologies and services and the elimination of redundancy. During the ISE phased implementation, ISC members will assess the potential impact of the ISE on the enterprise architectures and networks of participating agencies, all of which are required to be consistent with the Office of Management and Budget's (OMB) FEA

[33] For more information on the FEA process, go to http://www.whitehouse.gov/omb/egov/a-1-fea.html.

Framework. Specific implementation tasks, which tie to the Presidential Guidelines and Requirements (see Section 3.5), are identified below.

- Task 8.1: Identify All Major Enterprise Architectures and Networks Within the Counterterrorism Community. (Leads: PM, ISC, NSC, with support from OMB)

  Due Date: March 16, 2006 (ties to deliverable for Task 1.1, see Section 3.5.1)

  Deliverable: "As-Is" Inventory of Major Information Sharing Enterprise Architectures and Networks.

- Task 8.2: Develop an Enterprise Architecture Approach for Adopting Common Standards on Information Sharing. (Leads: PM, ISC with support from OMB/FEA PMO)

  Due Date: March 16, 2006 (ties to deliverable for Task 2.1, see Section 3.5.2)

  Deliverable: Enterprise Architecture Approach for the ISE.

- Task 8.3: Monitor, Oversee, and Evaluate Implementation. (Leads: OMB/FEA, PM, and Agency ISC Representatives)

  Due Date: Ongoing

  Deliverable: Enterprise Architecture Status Report (periodic report).

3.6.3 ISE Funding Strategy & Resource Requirements

Since defining the "As-Is" ISE and development of the environment is still underway, detailed funding recommendations are not appropriate at this time. However, there are steps necessary to notify agencies of likely future actions and to prepare for development of a comprehensive investment strategy.

To date, funding for programs and systems related to terrorism information often has been agency- or operating-division-specific, focused on addressing the various agency-unique mission requirements rather than serving a common government-wide goal. As a result, the Federal Government has spent billions of dollars on systems not designed explicitly to promote government-wide sharing. To maximize these investments, the environment will need to leverage these systems and the programs they support. In some instances, upgrades will be necessary to ensure the systems support the environment and meet common standards for sharing information. In FY2006 agencies have plans for new investments and other development, modernization or enhancements to existing technology investments.

To the greatest extent practicable, investments in current relevant systems should be consistent with plans to develop the proposed environment. As part of the FY2006 budget process, OMB notified agencies of its intent to work with them to ensure the investments supporting terrorism information sharing align with the Implementation Plan for the environment. In particular, agencies were alerted that their FY2006 funding might be redirected as needed to support the forthcoming Implementation Plan for the environment.

Many of these investments may be appropriate (i.e., they further the goal of terrorism information sharing and will support the environment within the mission context of the respective agency). However, in light of current plans for the environment, some investments may no longer represent the best use of resources, and others could conflict with the proposed efforts. Therefore, agencies must conduct thorough reviews of all current, new, and planned investments to ensure:

- New investments contemplated will not go forward if they conflict with the proposed direction of the environment, either by unnecessarily creating new barriers and redundancies, or by reinforcing existing barriers; and

- Resources for new systems and upgrades are planned and executed with the environment in mind.

For the purposes of achieving the ISE operating capability, the funding for development, modernization, or other enhancements to systems can be reviewed for opportunities to support implementation. However, a comprehensive investment strategy is essential to achieve the environment. This strategy will be fully developed as the plans for the environment advance. A critical part of this strategy will be an understanding of the current programs and IT investments that support terrorism information sharing. Therefore, the current inventory of systems and programs should continue to be refined to identify and establish a baseline of the Federal Government's investment in this area.

Due to the varying levels of maturity of each ISE participant's IT infrastructure, it is not possible to accurately determine the overall cost to the nation to fully implement an interoperable terrorism information sharing environment without collecting and analyzing additional information. Therefore, each ISE participant must:

- Identify the resources required for the establishment of the proposed interoperable terrorism information sharing environment;
- Identify and, as appropriate, recommend the consolidation and elimination of current programs, systems, and processes used to share terrorism information that are not consistent with the environment; and
- Recommend, as appropriate, the redirection of existing resources to support the environment.

The PM, with support from OMB and the ISC, will have responsibility for developing the overall investment strategy. The investment strategy will be described in the comprehensive Implementation Plan.

The PM, with support from OMB and the ISC, will undertake the following to develop the ISE funding strategy:

- Task 9.1: Identify Stakeholder Agencies' FY2006 and FY2007 Portfolios. (Lead: PM with OMB and ISC support)

  Due Date: March 16, 2006

  Deliverable: Baseline ISE Investment Portfolio.

- Task 9.2: Develop ISE investment strategy. (Lead: PM with OMB and ISC support)

  Due Date: June 14, 2006

  Deliverable: Overall ISE investment strategy.

- Task 9.3: Define "Quick Wins" Budget Recommendations. (Lead: PM with OMB and ISC support)

  Due Date: June 14, 2006

  Deliverable: Budget Recommendations for FY2006 Reprogramming and FY2007 Budget Amendment Proposals *(as appropriate).*

- Task 9.4: Review FY2008 Investments. (Lead: ODNI, PM with OMB and ISC support)

  Due Date: September 25, 2006

  Deliverable: FY2008 Investment Review Process Management.

- Task 9.5: Approve FY2008 ISE Portfolio. (Lead: PM with OMB and ISC support)

  Due Date: January 5, 2007

  Deliverable: Recommendations to Departments, Agencies and OMB for FY2008 ISE Portfolio *(PM will report consolidated ISE Portfolio).*

3.6.4 Performance Measurement

A comprehensive performance measurement strategy will allow the Executive Branch to routinely and consistently evaluate government-wide performance with regard to information sharing. Through the implementation and ongoing capture of performance measures to assess the ISE's compliance with its strategic goals and objectives, leaders will have incremental views into the success of information sharing initiatives across agency and jurisdictional boundaries and between the Federal departments and agencies and State, local, and tribal governments and private sector entities. Leaders will have tools and techniques by which they can assess the status of the ISE and refine and revise policies and directives as necessary. A four-step approach guides the development of this performance measurement strategy as well as the design of specific information sharing performance measures.

- Task 10.1: Design Performance Measurement Scope and Focus. (Leads: PM, ISC)

  Due Date: March 16, 2006

  Deliverable: Performance Measurement Targets, Timelines and Action Plan.

- Task 10.2: Develop and Test Performance Measures. (Leads: PM, ISC)

  Due Date: June 14, 2006

  Deliverable: Strategic and Operational Performance Measures

- Task 10.3: Implement Performance Management Program. (Lead: Federal departments and agencies in coordination with the PM and ISC)

  Due Date: June 14, 2006 (ties to Task 7.2, see Section 3.5.7)

  Deliverable: Implementation Results and Ongoing Measurement Timetable.

- Task 10.4: Develop First ISE Performance Management Report. (Leads: PM and ISC with data provided by Federal departments and agencies)

  Due Date: December 16, 2006

  Deliverable: ISE Performance Management Report as required by IRTPA Section 1016(f).

- Task 10.5: Periodically Review and Adjust Performance Measures to Ensure They Continue to Meet ISE Performance Management Needs. (Leads: PM and ISC with data provided by Federal departments and agencies)

  Due Date: Ongoing

  Deliverable: Revised Strategic and Operational Performance Measures

3.6.5 Electronic Directory Services

Section 1016 of IRTPA mandates that the ISE provide Electronic Directory Services (EDS), or the functional equivalent, to enable authorized participants to locate and access information, organizations, services and personnel in support of their respective mission requirements for terrorism information. The EDS will enable authorized users, including operators, analysts,

responders, planners and policy makers, to locate and access information, organizations, services and personnel in support of their respective mission requirements. This includes finding experts and possible collaboration partners.

Several directory services currently exist within individual ISE communities that provide working models for the end-state EDS. In deploying EDS, the PM and ISC will leverage these existing directory systems to the maximum possible extent. In addition, EDS must ensure that its services are available across domains and security levels.

- Task 11.1: Deploy Initial Capability for Electronic Directory Services. (Leads: PM, ISC)

  Due Date: March 31, 2006

  Deliverable: Initial capability for an EDS or functional equivalent.

4 Required Program Manager Recommendations

As discussed in Section 3.4.1, IRTPA assigns the Program Manager the responsibility, in consultation with the ISC, to provide two recommendations in the Implementation Plan Report:

- Requirement 9 - Whether, and under what conditions, the ISE should be expanded to include other intelligence information; and
- Requirement 11 - A future management structure for the ISE, including whether the position of the PM should continue to remain in existence.

These required recommendations are discussed below and will be detailed in the comprehensive Implementation Plan for the ISE, expected to be submitted to the Congress in July 2006.

Given the incremental and iterative implementation approach to achieve the vision of the ISE, the PM recognizes that the expansion of the ISE to encompass information pertaining to missions other than counterterrorism may be a long-range goal, achievable after establishment of an effective ISE framework that focuses on terrorism information. While the immediate focus of the ISE is terrorism information, the implementation approach will in no way preclude the development or leveraging of systems, policies, and business processes that better enable Federal, State, local, and tribal governments and the private sector to better share all relevant information.

The PM's Office will be essential to the implementation of the ISE and until such time that the ISE communities are systematically executing the ISE vision. The PM will be required to continually update and keep Congress informed of the progress made to enhance information sharing. Additionally, for purposes of budget planning and programming, the DNI and PM will work with the Congress to periodically calibrate requirements for the PM position in support of the development and implementation of the ISE now and into the future. As stated above, the future management structure of the ISE will be recommended in the July 2006 report to Congress.

5 Conclusion

Designing and implementing the ISE is a complex undertaking. It involves integrating the unique information requirements of the individual communities into a comprehensive and coordinated structure. To establish an effective ISE, significant challenges across many areas of policy, operations and technology must be surmounted. Moreover, the ISE will be structured to flexibly adapt to changing terrorist threats and information requirements.

Despite the challenges, implementing the ISE is an attainable goal—in fact, the realities of our time demand success in this endeavor. This Interim Implementation Plan highlights a national vision for designing and implementing a comprehensive, integrated and coordinated ISE and describes the incremental steps necessary for success. The resulting ISE will make available fast, accessible, accurate and timely terrorism information, tools and capabilities to those who need them.

Tab A: Cross-References to Requirements of Intelligence Reform and Terrorist Prevention Act of 2004

IRTPA Requirement (Section 1016(e))		Cross-References
1	A description of the functions, capabilities, resources and conceptual design of the ISE, including standards.	Sections 3.1, 3.5.1, 3.5.2 and 3.6.1
2	A description of the impact on enterprise architectures of participating agencies.	Section 3.6.2
3	A budget estimate that identifies the incremental costs associated with designing, testing, integrating, deploying, and operating the ISE.	Section 3.6.3
4	A project plan for designing, testing, integrating, deploying, and operating the ISE.	Discussed in Section 3.4.2
5	The policies and directives referred to in subsection (b)(1)(C), as well as the metrics and enforcement mechanisms that will be utilized. (Note: Subsection (b)(1)(C) states that, in the establishment of the ISE, the President shall, "determine and enforce the policies, directives, and rules that will govern the content and usage of the ISE.")	Sections 3.5 and 3.6.4
6	Objective, system wide performance measures to enable the assessment of progress toward achieving the full implementation of the ISE.	Section 3.6.4
7	A description of the training requirements needed to ensure that the ISE will be adequately implemented and properly utilized.	Section 3.5.7
8	A description of the means by which privacy and civil liberties will be protected in the design and operation of the ISE.	Sections 3.3.4 and 3.5.6
9	The recommendations of the Program Manager, in consultation with the Information Sharing Council, regarding whether, and under what conditions, the ISE should be expanded to include other intelligence information.	Chapter 4
10	A delineation of the roles of the Federal departments and agencies that will participate in the ISE, including an identification of the agencies that will deliver the infrastructure needed to operate and manage the ISE (as distinct from individual department or agency components that are part of the ISE), with such delineation of roles to be consistent with – (a) the authority of the Director of National Intelligence under this title, and the amendments made by this title, to set standards for information sharing throughout the intelligence community; and (b) the authority of the Secretary of Homeland Security and the Attorney General and the roles of the Department of Homeland Security and the Attorney General, in coordinating with State, local and tribal officials and the private sector.	Sections 3.5.1 and 3.5.3
11	The recommendations of the program manager, in consultation with the ISC, for a future management structure or the ISE, including whether the position of program manager should continue to remain in existence.	Chapter 4

Tab B: December 16, 2005 Memorandum for the Heads of Executive Departments and Agencies

SUBJECT: Guidelines and Requirements in Support of the Information Sharing Environment

Ensuring the appropriate access to, and the sharing, integration, and use of, information by Federal, State, local, and tribal agencies with counterterrorism responsibilities, and, as appropriate, private sector entities, while protecting the information privacy and other legal rights of Americans, remains a high priority for the United States and a necessity for winning the war on terror. Consistent with section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108 458) (IRTPA), my Administration is working to create an Information Sharing Environment (ISE) to facilitate the sharing of terrorism information (as defined in Executive Order 13388 of October 25, 2005).

Section 1016 of IRTPA supplements section 892 of the Homeland Security Act of 2002 (Public Law 107 296), Executive Order 13311 of July 29, 2003, and other Presidential guidance, which address various aspects of information access. On April 15, 2005, consistent with section 1016(f) of IRTPA, I designated the program manager (PM) responsible for information sharing across the Federal Government. On June 2, 2005, my memorandum entitled "Strengthening Information Sharing, Access, and Integration - Organizational, Management, and Policy Development Structures for Creating the Terrorism Information Sharing Environment" directed that the PM and his office be part of the Office of the Director of National Intelligence (DNI), and that the DNI exercise authority, direction, and control over the PM and ensure that the PM carries out his responsibilities under IRTPA. On October 25, 2005, I issued Executive Order 13388 to facilitate the work of the PM and the expeditious establishment of the ISE and restructure the Information Sharing Council (ISC), which provides advice concerning and assists in the establishment, implementation, and maintenance of the ISE.

On June 2, 2005, I also established the Information Sharing Policy Coordination Committee (ISPCC), which is chaired jointly by the Homeland Security Council (HSC) and the National Security Council (NSC), and which has the responsibilities set forth in section D of Homeland Security Presidential Directive 1 and other relevant presidential guidance with respect to information sharing. The ISPCC is the main day-to-day forum for interagency coordination of information sharing policy, including the resolution of issues raised by the PM, and provides policy analysis and recommendations for consideration by the more senior committees of the HSC and NSC systems and ensures timely responses.

Section 1016(d) of IRTPA calls for leveraging all ongoing efforts consistent with establishing the ISE, the issuance of guidelines for acquiring, accessing, sharing, and using information in support of the ISE and for protecting privacy and civil liberties in the development of the ISE, and the promotion of a culture of information sharing. Consistent with the Constitution and the laws of the United States, including section 103 of the National Security Act of 1947, as amended, and sections 1016 and 1018 of IRTPA, I hereby direct as follows:

1. Leveraging Ongoing Information Sharing Efforts in the Development of the ISE. The ISE shall build upon existing Federal Government policies, standards, procedures, programs, systems, and architectures (collectively "resources") used for the sharing and integration of and access to terrorism information, and shall leverage those resources to the maximum extent practicable, with the objective of establishing a decentralized, comprehensive, and coordinated environment for the sharing and integration of such information.

> a. The DNI shall direct the PM to conduct and complete, within 90 days after the date of this memorandum, in consultation with the ISC, a comprehensive evaluation of existing resources pertaining to terrorism information sharing employed by individual or multiple executive departments and agencies. Such evaluation shall assess such resources for

their utility and integrative potential in furtherance of the establishment of the ISE and shall identify any unnecessary redundancies.

b. To ensure that the ISE supports the needs of executive departments and agencies with counterterrorism responsibilities, and consistent with section 1021 of IRTPA, the DNI shall direct the PM, jointly with the Director of the National Counterterrorism Center (NCTC), and in coordination with the heads of relevant executive departments and agencies, to review and identify the respective missions, roles, and responsibilities of such executive departments and agencies, both as producers and users of terrorism information, relating to the acquisition, access, retention, production, use, management, and sharing of terrorism information. The findings shall be reviewed through the interagency policy coordination process, and any recommendations for the further definition, reconciliation, or alteration of such missions, roles, and responsibilities shall be submitted, within 180 days after the date of this memorandum, by the DNI to the President for approval through the Assistant to the President for Homeland Security and Counterterrorism (APHS-CT) and the Assistant to the President for National Security Affairs (APNSA). This effort shall be coordinated as appropriate with the tasks assigned under the Guidelines set forth in section 2 of this memorandum.

c. Upon the submission of findings as directed in the preceding paragraph (1(b)), the DNI shall direct the PM, in consultation with the ISC, to develop, in a manner consistent with applicable law, the policies, procedures, and architectures needed to create the ISE, which shall support the counterterrorism missions, roles, and responsibilities of executive departments and agencies. These policies, procedures, and architectures shall be reviewed through the interagency policy coordination process, and shall be submitted, within 180 days after the submission of findings as directed in the preceding paragraph (1(b)), by the DNI to the President for approval through the APHS-CT and the APNSA.

2. Information Sharing Guidelines. Consistent with section 1016(d) of IRTPA, I hereby issue the following guidelines and related requirements, the implementation of which shall be conducted in consultation with, and with support from, the PM as directed by the DNI:

a. Guideline 1 - Define Common Standards for How Information is Acquired, Accessed, Shared, and Used Within the ISE

The ISE must, to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE consistent with the protection of intelligence, law enforcement, protective, and military sources, methods, and activities.

Consistent with Executive Order 13388 and IRTPA, the DNI, in coordination with the Secretaries of State, Defense, and Homeland Security, and the Attorney General, shall develop and issue, within 90 days after the date of this memorandum, common standards (i) for preparing terrorism information for maximum distribution and access, (ii) to enable the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE while safeguarding such information and protecting sources and methods from unauthorized use or disclosure, (iii) for implementing legal requirements relating to the handling of specific types of information, and (iv) that include the appropriate method for the Government-wide adoption and implementation of such standards. Such standards shall accommodate and reflect the sharing of terrorism information, as appropriate, with State, local, and tribal governments, law enforcement agencies, and the private sector. Within 90 days after the issuance of such standards, the Secretary of Homeland Security and the Attorney General shall jointly disseminate such standards for use by State, local, and tribal governments, law enforcement agencies, and the private sector, on a mandatory basis where possible and a voluntary basis where not.

The DNI may amend the common standards from time to time as appropriate through the same process by which the DNI issued them.

b. Guideline 2 - Develop a Common Framework for the Sharing of Information Between and Among Executive Departments and Agencies and State, Local, and Tribal Governments, Law Enforcement Agencies, and the Private Sector

Recognizing that the war on terror must be a national effort, State, local, and tribal governments, law enforcement agencies, and the private sector must have the opportunity to participate as full partners in the ISE, to the extent consistent with applicable laws and executive orders and directives, the protection of national security, and the protection of the information privacy rights and other legal rights of Americans.

Within 180 days after the date of this memorandum, the Secretary of Homeland Security and the Attorney General, in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI, and consistent with the findings of the counterterrorism missions, roles, and responsibilities review under section 1 of this memorandum, shall:

(i) perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing with State, local, and tribal governments, law enforcement agencies, and the private sector; and

(ii) submit to the President for approval, through the APHS-CT and the APNSA, a recommended framework to govern the roles and responsibilities of executive departments and agencies pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and among such departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities.

c. Guideline 3 - Standardize Procedures for Sensitive But Unclassified Information

To promote and enhance the effective and efficient acquisition, access, retention, production, use, management, and sharing of Sensitive But Unclassified (SBU) information, including homeland security information, law enforcement information, and terrorism information, procedures and standards for designating, marking, and handling SBU information (collectively "SBU procedures") must be standardized across the Federal Government. SBU procedures must promote appropriate and consistent safeguarding of the information and must be appropriately shared with, and accommodate and reflect the imperative for timely and accurate dissemination of terrorism information to, State, local, and tribal governments, law enforcement agencies, and private sector entities. This effort must be consistent with Executive Orders 13311 and 13388, section 892 of the Homeland Security Act of 2002, section 1016 of IRTPA, section 102A of the National Security Act of 1947, the Freedom of Information Act, the Privacy Act of 1974, and other applicable laws and executive orders and directives.

(i) Within 90 days after the date of this memorandum, each executive department and agency will conduct an inventory of its SBU procedures, determine the underlying authority for each entry in the inventory, and provide an assessment of the effectiveness of its existing SBU procedures. The results of each inventory shall be reported to the DNI, who shall provide the compiled results to the Secretary of Homeland Security and the Attorney General.

(ii) Within 90 days after receiving the compiled results of the inventories required under the preceding paragraph (i), the Secretary of Homeland Security and the Attorney General, in coordination with the Secretaries of State, Defense, and Energy, and the DNI, shall submit to the President for approval recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information in the manner described in paragraph (iv) below.

(iii) Within 1 year after the date of this memorandum, the DNI, in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General, and in consultation with all other heads of relevant executive departments and agencies, shall submit to the President for approval recommendations for the standardization of SBU procedures for all types of information not addressed by the preceding paragraph (ii) in the manner described in paragraph (iv) below.

(iv) All recommendations required to be submitted to the President under this Guideline shall be submitted through the Director of the Office of Management and Budget (OMB), the APHS-CT, and the APNSA, as a report that contains the following:

> (A) recommendations for government-wide policies and procedures to standardize SBU procedures;
>
> (B) recommendations, as appropriate, for legislative, policy, regulatory, and administrative changes; and
>
> (C) an assessment by each department and agency participating in the SBU procedures review process of the costs and budgetary considerations for all proposed changes to marking conventions, handling caveats, and other procedures pertaining to SBU information.

(v) Upon the approval by the President of the recommendations submitted under this Guideline, heads of executive departments and agencies shall ensure on an ongoing basis that such recommendations are fully implemented in such department or agency, as applicable. The DNI shall direct the PM to support executive departments and agencies in such implementation, as well as in the development of relevant guidance and training programs for the standardized SBU procedures.

d. Guideline 4 - Facilitate Information Sharing Between Executive Departments and Agencies and Foreign Partners

The ISE must support and facilitate appropriate terrorism information sharing between executive departments and agencies and foreign partners and allies. To that end, policies and procedures to facilitate such informational access and exchange, including those relating to the handling of information received from foreign governments, must be established consistent with applicable laws and executive orders and directives.

Within 180 days after the date of this memorandum, the Secretary of State, in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the DNI, shall review existing authorities and submit to the President for approval, through the APHS-CT and the APNSA, recommendations for appropriate legislative, administrative, and policy changes to facilitate the sharing of terrorism information with foreign partners and allies, except for those activities conducted pursuant to sections 102A(k), 104A(f), and 119(f)(1)(E) of the National Security Act of 1947.

e. Guideline 5 - Protect the Information Privacy Rights and Other Legal Rights of Americans

As recognized in Executive Order 13353 of August 27, 2004, the Federal Government has a solemn obligation, and must continue fully, to protect the legal rights of all Americans in the effective performance of national security and homeland security functions. Accordingly, in the development and use of the ISE, the information privacy rights and other legal rights of Americans must be protected.

(i) Within 180 days after the date of this memorandum, the Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information, shall (A) conduct a review of current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans, (B) develop guidelines designed to be implemented by executive departments and agencies to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE, including in the acquisition, access, use, and storage of personally identifiable information, and (C) submit such guidelines to the President for approval through the Director of OMB, the APHS-CT, and the APNSA. Such guidelines shall not be inconsistent with Executive Order 12333 and guidance issued pursuant to that order.

(ii) Each head of an executive department or agency that possesses or uses intelligence or terrorism information shall ensure on an ongoing basis that (A) appropriate personnel, structures, training, and technologies are in place to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans, and (B) upon approval by the President of the guidelines developed under the preceding subsection (i), such guidelines are fully implemented in such department or agency.

3. Promoting a Culture of Information Sharing. Heads of executive departments and agencies must actively work to create a culture of information sharing within their respective departments or agencies by assigning personnel and dedicating resources to terrorism information sharing, by reducing disincentives to such sharing, and by holding their senior managers and officials accountable for improved and increased sharing of such information.
Accordingly, each head of an executive department or agency that possesses or uses intelligence or terrorism information shall:

a. within 90 days after the date of this memorandum, designate a senior official who possesses knowledge of the operational and policy aspects of information sharing to (i) provide accountability and oversight for terrorism information sharing within such department and agency, (ii) work with the PM, in consultation with the ISC, to develop high level information sharing performance measures for the department or agency to be assessed no less than semiannually, and (iii) provide, through the department or agency head, an annual report to the DNI on best practices of and remaining barriers to optimal terrorism information sharing;

b. within 180 days after the date of this memorandum, develop and issue guidelines, provide training and incentives, and hold relevant personnel accountable for the improved and increased sharing of terrorism information. Such guidelines and training shall seek to reduce obstructions to sharing, consistent with applicable laws and regulations. Accountability efforts shall include the requirement to add a performance evaluation element on information sharing to employees' annual Performance Appraisal Review, as appropriate, and shall focus on the sharing of information that supports the mission of the recipient of the information; and

c. bring to the attention of the Attorney General and the DNI, on an ongoing basis, any restriction contained in a rule, regulation, executive order or directive that significantly impedes the sharing of terrorism information and that such department or agency head believes is not required by applicable laws or to protect the information privacy rights and other legal rights of Americans. The Attorney General and the DNI shall review such restriction and jointly submit any recommendations for changes to such restriction to the APHS-CT and the APNSA for further review.

4. Heads of executive departments and agencies shall, to the extent permitted by law and subject to the availability of appropriations, provide assistance and information to the DNI and the PM in the implementation of this memorandum.

5. This memorandum:

a. shall be implemented in a manner consistent with applicable laws, including Federal laws protecting the information privacy rights and other legal rights of Americans, and subject to the availability of appropriations;

b. shall be implemented in a manner consistent with the statutory authority of the principal officers of executive departments and agencies as heads of their respective departments or agencies;

c. shall not be construed to impair or otherwise affect the functions of the Director of the Office of Management and Budget relating to budget, administrative, and legislative proposals; and

d. is intended only to improve the internal management of the Federal Government and is not intended to, and does not, create any rights or benefits, substantive or procedural, enforceable at law or in equity by a party against the United States, its departments, agencies, or entities, its officers, employees, or agencies, or any other person.

GEORGE W. BUSH

Tab C: Due Dates of ISE Interim Implementation Plan Tasks

TASK	DESCRIPTION	LEAD	DELIVERABLES	DUE DATE
1.1	Comprehensive assessment of existing resources pertaining to terrorism information sharing employed by individual or multiple executive departments and agencies	PM, ISC	Report assessing existing resources for utility and integrative potential in furtherance of the establishment of the ISE and identification of unnecessary redundancies	March 16, 2006
2.1	Develop and issue common standards for preparing terrorism information for maximum distribution and access while safeguarding such information and protecting sources and methods from unauthorized use or disclosure.	DNI in coordination with Secretaries of State, Defense, and Homeland Security and the Attorney General	Government-wide, common standards that promote the maximum distribution of and access to terrorism information, including the appropriate method for government-wide adoption and implementation of these standards	March 16, 2006
4.1	Conduct an inventory of SBU procedures, determine the underlying authority for each entry in the inventory, and provide an assessment of the effectiveness of existing SBU procedures.	All Federal departments and agencies	Report to the DNI on SBU inventory results. The DNI will, in turn, provide the compiled results to the Secretary of Homeland Security and the Attorney General.	March 16, 2006
7.1	Designate a senior official to provide accountability and oversight for terrorism information sharing, work with the PM, in consultation with the ISC, to develop high-level information sharing performance measures for the department or agency to be assessed no less than semiannually, and provide, through the department or agency head, an annual report to the DNI on best practices of and remaining barriers to optimal terrorism information sharing.	Federal departments and agencies	Memorandum designating responsible official for each department or agency.	March 16, 2006
8.1	Identify All Major Enterprise Architectures and Networks Within the Counterterrorism Community.	PM, ISC, NSC, with support from OMB	"As-Is" Inventory of Major Information Sharing Enterprise Architectures and Networks.	March 16, 2006 (ties to Task 1.1)

TASK	DESCRIPTION	LEAD	DELIVERABLES	DUE DATE
8.2	Develop an Enterprise Architecture Approach for Adopting Common Standards on Information Sharing.	PM, ISC with support from OMB/FEA PMO	Enterprise Architecture Approach for the ISE.	March 16, 2006 (ties to Task 2.1)
9.1	Identify Stakeholder Agencies' FY2006 and FY2007 Portfolios	PM with OMB and ISC support	Baseline ISE Investment Portfolio	March 16, 2006
10.1	Design Performance Measurement Scope and Focus.	PM, ISC	Performance Measurement Targets, Timelines and Action Plan.	March 16, 2006
11.1	Deploy Initial Capability for Electronic Directory Services.	PM, ISC	Initial capability for an EDS or functional equivalent.	March 31, 2006
1.2	Review and identify missions, roles and responsibilities of executive departments and agencies relating to the acquisition, access, retention, production, use, management, and sharing of terrorism information.	PM, Director of NCTC in coordination with relevant departments and agencies	Findings and recommendations for the further definition, reconciliation, or alteration of counterterrorism missions, roles and responsibilities.	June 14, 2006
2.2	Disseminate these standards for use by State, local, and tribal governments, law enforcement agencies, and the private sector, on a mandatory basis where possible and a voluntary basis where not.	Secretary of Homeland Security and the Attorney General	Common standards for use by Federal, State, local, and tribal governments, law enforcement agencies, and the private sector.	June 14, 2006
3.1	Perform a comprehensive review of the authorities and responsibilities of executive departments and agencies regarding information sharing with State, local, and tribal governments, law enforcement agencies, and the private sector and recommend an appropriate sharing framework to the President.	Secretary of Homeland Security and the Attorney General in consultation with the Secretaries of State, Defense, and Health and Human Services, and the DNI	Recommended framework pertaining to the acquisition, access, retention, production, use, management, and sharing of homeland security information, law enforcement information, and terrorism information between and among Federal departments and agencies and State, local, and tribal governments, law enforcement agencies, and private sector entities.	June 14, 2006

TASK	DESCRIPTION	LEAD	DELIVERABLES	DUE DATE
4.2	Develop recommendations for the standardization of SBU procedures for homeland security information, law enforcement information, and terrorism information.	Secretary of Homeland Security and the Attorney General in coordination with the Secretaries of State, Defense, and Energy, and the DNI	Report to the President in accordance with provisions of paragraph 2.c.(iv) of December 16, 2005 Presidential memorandum.	June 14, 2006
5.1	Review existing authorities and develop recommendations for sharing terrorism information with foreign partners and allies.	Secretary of State in coordination with the Secretaries of Defense, the Treasury, Commerce, and Homeland Security, the Attorney General, and the DNI	Recommendations for appropriate legislative, administrative, and policy changes to facilitate the sharing of terrorism information with foreign partners and allies.	June 14, 2006
6.1	Review current executive department and agency information sharing policies and procedures regarding the protection of information privacy and other legal rights of Americans, and develop guidelines to ensure that the information privacy and other legal rights of Americans are protected in the development and use of the ISE.	Attorney General and the DNI, in coordination with the heads of executive departments and agencies that possess or use intelligence or terrorism information	Recommended guidelines for Presidential approval that ensure the information privacy and other legal rights of Americans are protected in the development and use of the ISE.	June 14, 2006
7.2	Develop and issue guidelines, provide training and incentives, and hold relevant personnel accountable for the improved and increased sharing of terrorism information.	Federal departments and agencies	Departmental or agency guidelines, training, and incentives for promoting a culture of information sharing, including a performance evaluation element on information sharing to employees' annual Performance Appraisal Review.	June 14, 2006
9.2	Develop ISE investment strategy.	PM with OMB and ISC support	Overall ISE investment strategy.	June 14, 2006
9.3	Define "Quick Wins" Budget Recommendations.	PM with OMB and ISC support	Budget Recommendations for FY2006 Reprogramming and FY2007 Budget Amendment Proposals *(as appropriate).*	June 14, 2006

TASK	DESCRIPTION	LEAD	DELIVERABLES	DUE DATE
10.2	Develop and Test Performance Measures.	PM, ISC	Strategic and Operational Performance Measures.	June 14, 2006
10.3	Implement Performance Management Program.	Federal departments and agencies in coordination with the PM and ISC	Implementation Results and Ongoing Measurement Timetable.	June 14, 2006 (ties to Task 7.2)
9.4	Review FY2008 Investments.	ODNI/PM with OMB and ISC support	FY2008 Investment Review Process Management.	September 25, 2006
9.5	Approve FY2008 ISE Portfolio.	PM with OMB and ISC support	Recommendations to Departments, Agencies and OMB for FY2008 ISE Portfolio.	November 15, 2006
1.3	Develop the policies, procedures, and architectures needed to create the ISE, which shall support the counterterrorism missions, roles, and responsibilities of executive departments and agencies.	PM, ISC	ISE policies, procedures, and architectures.	December 11, 2006
4.3	Develop recommendations for the standardization of SBU procedures for all types of information.	DNI in coordination with the Secretaries of State, the Treasury, Defense, Commerce, Energy, Homeland Security, Health and Human Services, and the Attorney General and in consultation with all other heads of relevant executive departments and agencies	Report to the President in accordance with provisions of paragraph 2.c.(iv) of December 16, 2005 Presidential memorandum.	December 16, 2006
10.4	Develop First ISE Performance Management Report.	PM and ISC with data provided by Federal departments and agencies.	ISE Performance Management Report as required by IRTPA Section 1016(f).	December 16, 2006
4.4	Ensure on an ongoing basis that Presidentially-approved recommendations are fully implemented in such department or agency, as applicable.	All departments and agencies with support of PM	Guidance and training programs for the standardized SBU procedures.	Ongoing

TASK	DESCRIPTION	LEAD	DELIVERABLES	DUE DATE
6.2	Ensure that guidelines developed in Task 6.1 are fully implemented.	All departments and agencies	Appropriate personnel, structures, training, and technologies to ensure that terrorism information is shared in a manner that protects the information privacy and other legal rights of Americans.	Ongoing
7.3	Bring to the attention of the Attorney General and the DNI any restriction contained in a rule, regulation, executive order or directive that significantly impedes the sharing of terrorism information.	Federal departments and agencies	Department or agency memorandum, if applicable.	Ongoing
8.3	Monitor and Oversee Implementation.	OMB/FEA PMO	Enterprise Architecture Compliance Report (periodic report).	Ongoing
10.5	Periodically Review and Adjust Performance Measures to Ensure They Continue to Meet ISE Performance Management Needs.	PM and ISC with data provided by Federal departments and agencies.	Revised Strategic and Operational Performance Measures.	Ongoing

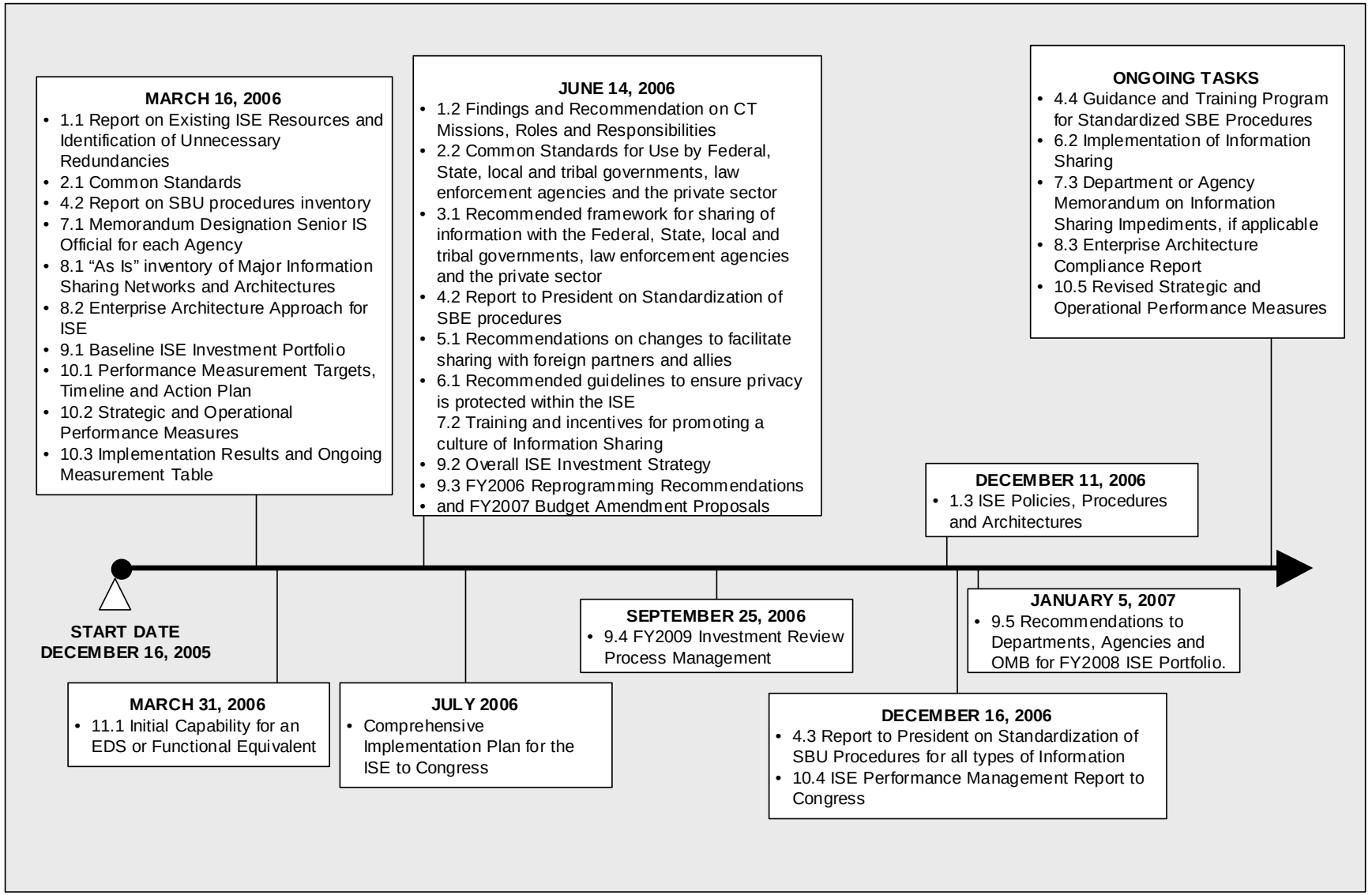

Figure C.1: ISE Implementation Tasks and Milestones